

## ⑫ 公開特許公報(A)

昭60-136440

⑤ Int.Cl.<sup>4</sup>  
H 04 L 9/02識別記号 庁内整理番号  
Z-7240-5K

⑬ 公開 昭和60年(1985)7月19日

審査請求 有 発明の数 1 (全 11 頁)

⑭ 発明の名称 セッション暗号キー更新方法

⑮ 特 願 昭59-243557

⑯ 出 願 昭59(1984)11月20日

優先権主張 ⑰ 1983年12月21日 ⑱ イギリス(GB) ⑲ 83307786.0

⑳ 発 明 者 クリストファー・ホラ ウエイ イギリス国エスグブリュー2、1アール・デイ、ロンドン、クリックルウッド、ソーヴァントン・ロード、ソーヴァントン・コート1番地

㉑ 出 願 人 インターナショナル・ビジネス・マシーンズ・コーポレーション アメリカ合衆国10504、ニューヨーク州アーモンク(番地なし)

㉒ 代 理 人 弁理士 頓宮 孝一 外1名

## 明 細 書

1. 発明の名称 セッション暗号キー更新方法

## 2. 特許請求の範囲

ホストデータプロセッサが通信ネットワークを介して各々検証モジュールを含む複数のメッセージ起点ユニットに接続され、各検証モジュールごとに取引きセッションキーを発行し記憶し、ユーザの入力装置で記憶されるユーザ識別番号と、ユーザが別に記憶している秘密番号と、から導出されるユーザ確認パラメータを各ユーザごとに発行し記憶するようなデータ通信システムにおいて、

(a) ユーザによつて取引きがメッセージ起点ユニットで開始されると、検証モジュールがユーザ識別番号と、現取引きセッションキーに基づくメッセージ確認コードと、を含む第1のメッセージを形成してホストデータプロセッサへ送るステップと、

(b) ホストデータプロセッサで第1のメッセージを受け取つてメッセージ確認コードを再生成し、

これと受信したメッセージ確認コードとを比較するステップと、

(c) ランダムキーを生成するステップと、

(d) ランダムキー、ユーザ確認パラメータ、および現取引きセッションキーに基づき新たな取引きセッションキーを生成するステップと、

(e) 現取引きセッションキーを用いて暗号化されたユーザ確認パラメータと、ユーザ確認パラメータを用いて暗号化されたランダムキーと、を含む第2のメッセージを形成して検証モジュールへ送るステップと、

(f) 検証モジュールでユーザの入力する秘密番号を受け取つてユーザ確認パラメータを再生成するステップと、

(g) 再生成されたユーザ確認パラメータと受信したユーザ確認パラメータとを比較してユーザの入力を検証し、これにより検証された正しいユーザ確認パラメータを用いてランダムキーを暗号解読し、ホストデータプロセッサに送られる次のメッセージのために使用される新たな取引きセッション

ンキーを生成し記憶するステップと、

を有することを特徴とするセッション暗号キー更新方法。

### 3. 発明の詳細な説明

#### 〔産業上の利用分野〕

本発明はデータ通信システムの安全保護の技術に関する。

#### 〔従来技術〕

金融取引に関するメッセージを伝えるデータ通信ネットワークは今日では広く一般に使用されるようになった。磁気ストライプカードと秘密番号(PIN)を有する銀行の顧客によつて操作され、遠隔のデータ処理機械にオンラインで接続される現金支払端末機は今やごくあたりまえのものとなつている。さらに、単に現金を支払うだけでなくより多くの機能を遂行することのできる自動現金預払機(ATM)が登場し、金融取引に関わる大量のペーパーワーク(小切手の処理など)

(3)

個人キー(KP)と会計番号(PAN)を記憶する。ユーザも個人識別番号(PIN)を有しそれを個人個人で覚えておく。

小売業者の端末に接続されたEFTモジュールにカードを入れると、取引が開始される。そうしてPANおよびセッションキー(KS)を含む要求メッセージがカード発行業者のデータ処理センターに送られる。カード発行業者は自身の記憶するKPおよびPINのバージョンならびに端末から受信した時間経過パラメータに基づいて確認パラメータ(TAP)を生成する。TAPは応答メッセージで端末に戻される。入力されたPINに基づき、カードに入っているPINおよびKPを部分的に処理することによつて得られたTAPと、端末に戻つてきたTAPを比較する。両者が一致すればそれは入力されたPINが有効であることを意味する。

要求メッセージはKSの下でコード化されたPANと定義域間キーの下でコード化されたKSを含む。メッセージ確認コード(MAC)が各メッ

(5)

を減じねばならないという経済的な要求に答えている。

小売業者がバケット交換網に接続された端末を有し、顧客が買物をしたときに借方の記入された勘定書を小売業者の端末からオンラインで受け取るようなPOS/EFT(Point of sale/electronic funds transfer)システムもまた開発されている。

英国特許出願第8324916号にはPOS/EFTシステムに関する記載がある。この特許出願にはさらにユーザおよびメッセージ確認検査用のシステムに関する記載もある。これらのシステムでは、店に設置された小売業者の端末が、公衆交換通信システムを介して、カード発行サービス機関のデータ処理センターに接続されるようなEFTシステムが記載されている。そのシステムのユーザには機密保持されたバンクカードが発行される。このカードはマイクロプロセッサ、ROS、およびRAMを有する。カードの発行業者がカードをユーザに発行する際、そのカードのROSに

(4)

ッセージに付加される。KSの下でコード化された項を含むメッセージにより受信されたMACと再生されたMACとで、受信されたKSが有効であることと、そのメッセージが有効な端末またはカードから発せられたものであることを示す。

EFTシステムには下記に示す幾つかの従来技術がある。

欧州特許公開第32193号はユーザおよび小売業者が、各々、暗号キー(小売業者のキー:Kr、ユーザのキー:Kp)を有し、この暗号キーがユーザの会計番号および小売業者の業務番号と共にホストCPUのデータ記憶装置に記憶されるようなシステムについて記載するものである。小売業者のキーKrおよびユーザのキーKpは、小売業者の取引用端末とホストCPUとの間で送られるデータを暗号化する際に用いられる。もちろん、ホストCPUに識別番号と暗号キーを有するユーザだけがこのシステムを利用できることは言うまでもない。しかしながらユーザの数が増えてくると、対応するキーおよび識別番号の検索に要する時間

(6)

はオンライン取引処理には到底容認できないようなものになる。しかもこのシステムは単一の定義域だけであり、個人識別番号(PIN)を使用しない。ユーザの識別の検証はホスト側で行われ、かつ、PINを用いないので、盗用されたカードが使用されてもこれを防ぐ手だてがない。

欧州特許公開第18129号は通信路上のデータの安全保障を図る方法について記載するものである。ユーザ識別コードまたは端末識別コードを主暗号キーと共に用いて、ダイヤル呼出し式データ通信ネットワークの守秘権および安全保障が提供される。有効な識別コードと主暗号キーとを対にしたもののリストがCPUに保持されている。CPUへ送られた識別コードと暗号キーの対はCPUに記憶されているコード対と比較される。両者が一致すればCPUは端末から送られてきたコード化されたデータを受諾する。ネットワークを介して送られる全てのデータは関係したユーザキーまたは端末キーを用いて暗号化され、許可されないアクセスは予防される。このシステムも単一

(7)

4ビット)を有するPINが必要になってくる。これは人間工学上は不利なものとなる。というのは、ユーザがそのような長い文字列を覚えておかなければならないのは面倒なことであるし、また文字列が長いためにそれを誤って入力してしまう確率も高くなるからである。ランダムな文字列は覚えにくいというので、ユーザが記憶し易いような文句をPINとして用いるとすれば、そのような文句は28文字程度は必要である。したがって、情報の記憶の問題がなくなつたとしても、依然として長い文字列の入力という人間工学上の問題は残る。

これまでに説明したシステムによつて可能となるEFTシステムは全てのユーザ(小売業者と顧客の両方)の勘定簿を保持するのは単一のホストCPUに限られている。

ところで多くのカード発行機関(銀行、クレジットカード会社等)が接続され、かつ電話交換機のような交換網を介して何百もの小売業者が接続されるEFTシステムは安全保障上多くの問題が

(9)

定義域であり、全ての端末キー(またはユーザキー)は中央ホスト側で認識しなければならない。この特許公開は多重ホスト環境について言及するものではない(交換問題について言及しない)。

英国特許出願第2052513A号はネットワーク(たとえば前記2つの欧州特許公開に示されるネットワーク)において局ごとに明らかな個人識別番号(PIN)のようなユーザ識別情報を伝送する必要をなくした装置および方法が記載されている。PINはユーザ局でランダムに生成された番号を用いてコード化され、ランダムに生成された番号およびコード化されたPINは処理局に送られる。処理局では、受信したこれらのランダム番号およびコード化されたPINを用いて、一般的に適用できる第2のPINがコード化され、この第2のPINと受信したPINとの比較により、受信したPINの有効性が判断される。このシステムは個人キーを使用しないので、これを十分に機密保持された安全保障システムにしようとすると、少なくとも14個のランダム文字(各々

(8)

ある。

国際公開WO81/02655号はエントリー端末でPINの暗号化が2回以上行われるような多重ホスト、多重ユーザシステムについて記憶するものである。取引の検証および許可に必要なデータがホストコンピュータに送られて、ホストコンピュータは暗号の解説に必要なデータを自身の記憶するデータベースからアクセスし、暗号化されたPINを含む取引を検証する。秘密の端末マスターキーは各端末で保管されねばならない。これらのマスターキーのリストはホストコンピュータ側にも保管されている。

カード発行機関の各ホストコンピュータで端末マスターキーのリストを保管するのは複雑なシステム(カード発行ホストで端末キーが管理されない、したがって、カード発行ホストで端末キーがわからないようなシステム)においては明らかに困難な作業である。

欧州特許公開第55580号はエントリー点である端末でPINの検証を行うことによつてネッ

(10)

トワークにおけるPIN情報の伝送の必要性をなくそうと意図するものである。これは銀行識別子(BIN)、ユーザの会計番号(ACCN)、およびPINオフセット番号が磁気ストライプにコード化されたカードを各ユーザに発行することによつて達成される。PIN、BIN、およびACCNからPINオフセットが計算される。ユーザは端末に接続されたキーボードからPINを入れる。端末はカードからもPINオフセット、BIN、およびACCNを読み取る。そうして端末はBIN、ACCN、およびユーザの入れたPINからPINオフセットを再び計算する。この再計算されたPINオフセットがカードから読み取られたPINオフセットと同じなら、そのPINは正しいと推定される。この手法はそのシステムが認証に関与しないという欠点と、PINオフセットがPIN、BIN、およびACCNから計算されるとわかれば、そのからくりを知つたものなら有効なPINを有する不正なカードを作ることができてしまうという欠点がある。

(11)

る。一意的なメッセージをPANと共にホストプロセッサに送り、そとでそのPANを用いて有効な許可パラメータ(VAP)を識別する。このVAPを用いてメッセージをコード化し、その結果(メッセージ確認コード:MAC)を取り引き端末に返す。端末はDAPを用いて同時に導出メッセージ確認コード(DMAC)を生成し、そのメッセージをコード化する。そうしてDMACとMACを比較し、その比較結果を用いてPINの有効性を判断する。

こうしたシステムではDAPおよびVAPの生成は短いPINだけに基づいて行われるので、暗号化に関して難点がある。その上、EFT端末は識別カードで伝えられる情報の全てをアクセスしなければならず、システムの安全保護の点からいっても問題である。

各定義域がデータプロセッサを含み、暗号化によつて機密保持された伝送が行われるような多重定義域通信ネットワークでは、定義域間キーを設けねばならない。定義域間キーを設けてそれを使

(13)

マイクロ回路チップ技術の発展により、今や、ユーザカードはユーザデータを磁気ストライプに記憶する代わりに、ROSを備えたマイクロプロセッサを包含できるようになった。マイクロプロセッサはカードをEFT端末に入れたときに活動化され、適切な電力供給のための接続およびデータ伝送インターフェースとの接続がなされる。カード上のマイクロプロセッサはそのROSに記憶された制御プログラムで制御される。ユーザの識別子および発行者の識別子もまた他の情報と共にROSに記憶されている。

このようなマイクロプロセッサを含むカードの例は英国特許出願第2081644A号および第2095175A号にある。

欧州特許出願第823069893号はPINがネットワークを介して間接的に伝送されるようなEFTネットワークの取り引き端末から入力されたPINの有効性を検査するための方法および装置について記載するものである。PINおよびPANを用いて許可パラメータ(DAP)を導出す

(12)

用するような通信安全保護システムは米国特許第4227253号に記載されている。ここに示される通信安全保護システムは各定義域がホストシステムと、それに関連するプログラムおよび通信端末の資源と、を有する多重定義域通信ネットワークの定義域間でデータを伝送するためのものである。ホストシステムおよび通信端末は複数のデータ安全保護装置を含む。データ安全保護装置は各々マスターキーを有する。これにより様々な暗号化オペレーションが可能となる。或る定義域のホストシステムが別の定義域のホストシステムと通信したいときは、両方のホストシステムで共通のセッションキーが設定され、暗号化オペレーションが可能となる。これは、両方のホストシステムでわかる互いに一致した定義域間キーを用いて達成される。しかしながら各ホストシステムは自身のマスターキーを相手側のホストシステムに明らかにする必要はない。定義域間キーは送信側のホストシステムにおいて1のキー(暗号化キー)の下で暗号化され、受信側のホストシステムにお

(14)

いては別のキー（別の暗号化キー）の下で暗号化される。送信側のホストシステムは暗号化されたセッションキーを生成して、送信側の定義域間キーの下で、セッションキーを再び暗号化し、これを相手のホストシステムに送信する。受信側のホストシステムは受信したセッションキーを定義域間キーの下での暗号から受信側のマスターキーの下での暗号に変換する（再暗号化する）。こうして両方のホストシステムで共通のセッションキーが使用できるようになるので、通信セッションが確立されて、これらのホストシステム間で暗号化オペレーションを進めることができる。

ホームバンキングシステムは顧客（ユーザ）の数が小規模である銀行のシステムとみなすことができる。システムのユーザには、たとえば、パーソナルコンピュータまたはキーボードを備えたテレビ受像機のような専用の端末装置が設置される。1組の装置が多数のユーザによつて共有されることもある。このシステムは個人的な情報へのアクセスの制御、一連の取引きの確認、およびそうし

(15)

れるユーザ確認パラメータを各ユーザごとに発行し記憶するようなデータ通信システムにおいて、

- (a) ユーザによつて取引きがメッセージ起点ユニットで開始されると、検証モジュールがユーザ識別番号と、現取引きセッションキーに基づくメッセージ確認コードと、を含む第1のメッセージを形成してホストデータプロセッサへ送るステップと、
- (b) ホストデータプロセッサで第1のメッセージを受け取つてメッセージ確認コードを再生成し、これと受信したメッセージ確認コードとを比較するステップと、
- (c) ランダムキーを生成するステップと、
- (d) ランダムキー、ユーザ確認パラメータ、および現取引きセッションキーに基づき新たな取引きセッションキーを生成するステップと、
- (e) 現取引きセッションキーを用いて暗号化されたユーザ確認パラメータと、ユーザ確認パラメータを用いて暗号化されたランダムキーと、を含む第2のメッセージを形成して検証モジュールへ送

(17)

た取引きの遂行の許可を保護するという安全保護上の要求を有する。

〔発明が解決しようとする問題点〕

以上説明したように従来技術におけるデータ通信システムは安全保護の点では未だ十分なものではない。

したがつて本発明の目的はデータ通信システムにおいてより優れた安全保護を提供することにある。

〔問題点を解決するための手段〕

本発明の目的は下記に示すセッション暗号キー更新方法を用いることによつて達成される。

ホストデータプロセッサが通信ネットワークを介して各々検証モジュールを含む複数のメッセージ起点ユニットに接続され、各検証モジュールごとに取りきセッションキーを発行し記憶し、ユーザの入力装置で記憶されるユーザ識別番号と、ユーザが別に記憶している秘密番号と、から導出さ

(16)

るステップと、

- (f) 検証モジュールでユーザの入力する秘密番号を受け取つてユーザ確認パラメータを再生成するステップと、
- (g) 再生成されたユーザ確認パラメータと受信したユーザ確認パラメータとを比較してユーザの入力を検証し、これにより検証された正しいユーザ確認パラメータを用いてランダムキーを暗号解読し、ホストデータプロセッサに送られる次のメッセージのために使用される新たな取引きセッションキーを生成し記憶するステップと、

を有することを特徴とするセッション暗号キー更新方法。

〔実施例〕

本実施例はホームバンキングシステムで使用される安全保護技術に関する。公衆交換システム（PSS）を介して顧客に接続される銀行のデータ処理センターは端末から受け取つたメッセージが有効な装置（銀行が許可した装置であつて、かつ、

(18)

そのユーザが有効なユーザである装置)から来たものであるかどうかを知る必要がある。

良好な実施例ではメッセージの起点ユニットとなる端末ごとに検証モジュールが存在する。検証モジュールは端末間で持ち運び可能である。各検証モジュールには検証モジュール識別子(VMID)、シード番号(VMSEED<sub>n</sub>)、初期取引キー(VMKEY<sub>n</sub>)、銀行識別アドレス(HIDD)およびインデックス番号(VMNDX)が発行される。銀行はVMIDによつて指標付けされるこれら全てを記憶する。ユーザが取引きを開始すると、端末はVMKEY<sub>n</sub>を用いて生成されたメッセージ確認コード(MAC1)を含み、VMIDおよびユーザ識別子UIDを有する第1のメッセージを構成する。

銀行は各ユーザに対してユーザ識別子(UID)およびユーザ秘密番号(UPW)を有する。これらは他の適用例でいうとPANおよびPINと等価なものである。銀行のデータ処理センターは第1のメッセージを受け取ると、VMIDを用いて

(19)

説しVMKEY<sub>n+1</sub>およびVMSEED<sub>n+1</sub>の自身バージョンを再び生成することができる。こうして新しい取引セッションキー(VMKEY<sub>n+1</sub>)とシード(VMSEED<sub>n+1</sub>)とを用いて端末から送られる次のメッセージを確認する。

このシステムを用いるならば部外者は検証モジュールをエミュレートすることはできない。すなわち検証モジュールの処理のたびごとに重要なパラメータ(VMKEYおよびVMSEED)を更新できるような銀行を装うことはできない。したがつて優れた安全保障システムを提供することができる。

本発明は1つのメッセージの伝送のためにだけ用いられるキーの下で暗号化された確認パラメータ(UPP)自身を利用することによつて、安全保障上、セッションキーを更新する、各検証モジュールの有効性を確認する、ホストの有効性を確認する、という特徴を含む。

第1図を参照してホームバンキングシステムの

(21)

VMKEY<sub>n</sub>の自身のバージョンを獲得して、MAC1を再び生成する。こうして再生成されたMAC1と受信したMAC1とを比較する。このオペレーションが成功すると、ランダムキー(RNKEY)が生成され、VMIDと共にRNKEYおよびVMSEED<sub>n</sub>を用いて新しい取引セッションキー(VMKEY<sub>n+1</sub>)が生成される。RNKEYおよびVMSEED<sub>n</sub>を用いて新しいVMSEED<sub>n+1</sub>もまた生成される。

VMSEED<sub>n</sub>およびVMKEY<sub>n</sub>を用いて暗号化された、UIDおよびUPWに基づく確認パラメータ(UPP)を含む第2のメッセージ(MSG2)が生成される。これをUAP(ユーザ確認パラメータ)と呼ぶ。このメッセージはUPP、VMSEED<sub>n</sub>、およびVMIDを用いて暗号化されたRNKEYも含む。

端末がMSG2を受け取つて、ユーザがUPW(PIN)を入力すると、端末はUPPを再び生成して、これと受信され暗号解読されたUPPとを比較する。端末はそれからRNKEYを暗号解

(20)

概略を説明する。

銀行および同様な金融機関のホストプロセス10は適切なインターフェースを介して公衆パケット交換網(PSS)12のような通信媒体に接続される。このシステムのユーザ(顧客)は端末機14を介してPSS12と対話する(端末機14はPSS12に接続される)。

端末機14はパーソナルコンピュータ、ビデオテックスシステムとして使用されるようなキーボード付テレビ受像機、または他の適切な入/出力表示装置でもよい。端末機14はモデムを介してPSS12に直接接続してもよいし、第1図に示すような局所ノード16を介してPSS12に接続してもよい。本発明を利用するホームバンキングシステムの各端末機は検証モジュール(VALMOD)と相互接続できる。

検証モジュールは、知能機密保護カード、携帯用PINPAD、完全な端末機、または端末機に設けられた論理モジュールを含む様々な物理装置の1つである。

(22)

第2図は良好な実施例で使用されるホストプロセッサ10の構成を示す図である。ホストプロセッサ10は制御ユニット20を有する。制御ユニット20はオペレーション制御用のマイクロコードを含む。記憶部21は送受モジュール22に接続される。記憶部12は外部ディスク記憶装置またはその他同様な装置でもよい。送受モジュール22は、それ自身、通信媒体(第1図ではPSS12)に接続されたモデムを含んでもよい。確認メッセージ生成器23、ランダム番号生成器24、取引キー生成器25、メッセージ構成レジスタ26、および暗号化/暗号解読(E/D)ユニット27は共通のバスを介して記憶部21および制御ユニット20へ接続される。入力メッセージは記憶部21へ直接に経路指定され、出力メッセージはメッセージ構成レジスタ26から直接に送信されるかまたは記憶部21を介して送信される。

もちろん多重プロセッサにおいては、第2図に示すユニットは、制御プログラムがオペレーテ

(23)

の発行者のシステム、たとえば銀行の支店、と対話したいときにそれができるような場所に検証モジュール(VA LMOD)を発行する。したがってVA LMODは多数の顧客で共有できる(異なる場所を移動できる)。顧客は金融機関によつて発行されるどのモジュールでも使用可能である。その機関のホストシステムのところのデータをアクセスする必要のある顧客にはユーザ識別番号(UID)およびユーザ用の秘密の合言葉(UPW)が与えられる。その顧客は必ずその機関によつて発行された検証モジュールを使用しなければならない。銀行の場合は、UIDは個人会計番号(PAN)と等価でありUPWは個人識別番号(PIN)と等価である。

#### 検証モジュールの発行

VA LMODは下記の情報を記憶する。

- (a) VA LMOD識別子(VMID)
- (b) 秘密の16進データ値(VMSEED<sub>n</sub>)
- (c) 秘密の暗号キー(VMKEY<sub>n</sub>)

(25)

ングシステムの優先度に応じてタスクをレジスタおよび処理ユニットに割り振るようにする限りは、個別に識別可能でなくてもよい。

第3図は検証モジュール14の構成を示す図である。検証モジュール14はマイクロプロセッサ30、RAM31、ROM32を含む。ROM32は検証モジュールおよび暗号化/暗号解読(E/D)ユニット33のための制御用マイクロコードを有する。共通のバスが以上の各ユニットを送受ユニット34に接続する。メッセージは送受ユニット34へ送られる前に初めに生成されRAM31に記憶される。受信メッセージはユニットがそれに作用する前に記憶される。

検証モジュールそれ自体は第3図に示す構成要素を全て含んでいる必要はない。たとえば送受ユニット34およびマイクロプロセッサ30は、取引の行われる、その検証モジュールに接続される端末機のユニットであつてもよい。

次にこのシステムの動作について説明する。銀行または金融機関は顧客(または顧客がその特定

(24)

(d) セロにセットされたインデックス番号(VMNDX = n)

(e) ユーザのホストの識別子(HIID)、これはたとえばPSSのユーザアドレスである。

以上の情報はVMIDで指標付けられるホスト側にも記憶されている。VMSEED<sub>n</sub>は、通常、データ暗号キーDKEYの下でEDKEY(VMSEED<sub>n</sub>)の形に暗号化することによつてホスト側で保護される。VMKEY<sub>n</sub>はホスト側でホストマスターキーの下でEHMKO(VMKEY<sub>n</sub>)の形に暗号化され記憶される。

UIDはその機関によつて決定されユーザデータバンクへのインデックスとして働く。UPWはその特定のUIDと共に用いる、機関によつて生成されるランダムな値である。UIDおよびUPWは各ユーザへ内密に供給される。この2つの値を組み合わせて8つの16進バイトから成るユーザ確認パラメータ(UPV)を構成する。この組合せの形式は、情報が失われない限りは、重要ではなく、その機能は要求に応じて造り替えることが

(26)

できる。UVPは $E_{HMKO}(UVP)$ の形で暗号キーとしてホスト側に記憶され、UIDにより指図される。

#### システムの使用法

1. ユーザはVALMODのある所へ行き自身のUIDを与えて(たとえば磁気ストライプカードまたはキーボードを介して)、VALMODはこのUIDを記憶する。
2. VALMODはHIID、VMID、VMPEAR(VMNDXのバリティに応じて0または1の値をとる)、およびUIDを有するMSG1を含むメッセージをコンパイルする。
3. VALMODはVMKEY<sub>n</sub>を用いてMSG1のためのメッセージ確認コードMAC1を生成する。
4. MSG1、MAC1が発行者に送られる。
5. VMNDXのバリティが正しければ、発行者は受信したMSG1および記憶されたVMKEY<sub>n</sub>を用いて(さもなければ前の値VMKEY<sub>n-1</sub>

(27)

MAC2を付加する。

8. 発行者はMSG2およびMAC2をVALMODに送る。VALMODは記憶されたVMKEY<sub>n</sub>を用いてMAC2を検証する。MAC2が不当なものであれば取引きは打ち切られる。
9. VALMODはユーザのUPWを要求する。このUPWと記憶されたUIDとを組み合わせて検証されるべきUVPを生成する。
10. VALMODは6cに示すようにUVPおよび記憶されたVMKEY<sub>n</sub>を用いて参照となるUAPを生成する。このUAPが受信したUAPと同じでないときは、取引きは打ち切られる。
11. VALMODは6dに示すように検証されたUVPおよび記憶されたVMSEED<sub>n</sub>を用いてUAKKEYを生成する。VALMODはUAKKEYを用いて受信したNEWKEYを暗号解読してRNKEYを得る。
12. VALMODは6aおよび6bに示すように記憶されたVMSEED<sub>n</sub>および受信したRNKEYを用いてVMSEED<sub>n+1</sub>およびVMKEY

(29)

およびVMSEED<sub>n-1</sub>を用いて)。参照となるMAC1を生成する。こうして生成したMAC1が受信したMAC1と同じでないときは、取引きは打ち切られる。

6. MAC1が有効ならば発行者はUIDを検査し、この検査が有効ならば発行者は暗号キーRNKEYをランダムに生成する。

- a)  $VMSEED_{n+1} = E_{RNKEY}(VMSEED_n)$
- b)  $VMKEY_{n+1} = D_{RNKEY}(VMSEED_n + VMID)$
- c)  $UAP = E_{VMKEY_n}(E_{UVP}(VMSEED_n))$
- d)  $UAKKEY = E_{VMKEY_n}(E_{UVP}(VMSEED_n + VMID))$
- e)  $NEWKEY = E_{UAKKEY}(RNKEY)$

発行者はa)およびb)を記憶し、d)を除く。

7. 発行者はUAPおよびNEWKEYを含むメッセージMSG2をコンパイルし、VMKEY<sub>n</sub>を用いてMSG2のためのメッセージ確認コード

(28)

$Y_{n+1}$ を生成する。VMSEED<sub>n+1</sub>およびVMKEY<sub>n+1</sub>はVMSEED<sub>n</sub>およびVMKEY<sub>n</sub>の代わりにVALMODに置かれ、VMNDXが1だけ増分される。

13. VALMODはMSG1の内容を含む確認メッセージMSG3を生成し、VMKEY<sub>n+1</sub>を用いてMSG3のためのメッセージ確認コードMAC3を付加する。これが発行者に送られる。
14. 発行者はこれを受け取るとVMKEY<sub>n+1</sub>を用いてMAC3を検証する。MAC3が不当なものであれば取引きは打ち切れ、VALMODは同期外れが通告される(再発行されるまではそれを使用することができない)。
15. 発行者は適切なキーの下で暗号化されたVMSEED<sub>n+1</sub>およびVMKEY<sub>n+1</sub>でVMSEED<sub>n</sub>およびVMKEY<sub>n</sub>を置き換える。

以上に示したオペレーションから言えることは、VALMODは下記の条件の場合にのみ秘密のデータを発行者と同期して変更するというのである。



a) VALMODは有効であつて既に同期化されている。

b) ユーザは有効かつ確認されている。

これらの条件を満たすことについての吟味はMAC3を用いて行われる。

VALMODおよび発行者の間でメッセージを記録するので、部外者はVALMODをエミュレートすることはできない。すなわち部外者は、VALMODを扱うたびに重要なパラメータ(VMSEEDおよびVMKEY)を更新するような発行者を装うことはできない。したがつて優れた安全保護システムが提供される。

MSG3を受け取ることによつてユーザデータおよび機構を正当に所有するユーザに、ユーザ自身の端末機を介して発行者ホストからアクセスできるようにする。一辺の為替取引きは端末のユーザによつて遂行され検査される。この通信はVMKEY<sub>n+1</sub>を用いてMAC3を生成することによつて確認される。

所望の全ての作業が完了するとき、為替取引

きを行う顧客の承認を得る必要がある。これは“完了”メッセージを発行者に送ることによつてなされる。こうしてPIN(UPW)の再エントリを含む別のVALMODシーケンスが繰り返される。

VMKEY<sub>n+2</sub>(新たに承諾されたもの)を用いて確認されたMSG3を受け取るのは、処理する発行者の権限である。VMKEY<sub>n+3</sub>でこれが確認され、その肯定応答がユーザの端末機に返される。

下記に示す表は取引セッションのオペレーションの間、および検証に関するメッセージ(MSG1、MSG2、およびMSG3)の形成の間に、VALMOD側およびホストプロセッサ側で記憶され生成される項目を示すことによつて、これまでに説明した手法を簡略的に表わすものである。

(31)

(32)

VALMOD側	ホスト側
記憶されるもの	記憶されるもの
VMID	VMID
VMSEED <sub>n</sub>	VMSEED <sub>n</sub>
VMKEY <sub>n</sub>	VMKEY <sub>n</sub>
VMNDX	VMNDX
HIID	UID
HIID	UVP
入力されるもの	
UID	
HIID、VMID、VMPAR(VMNDXに基づく)、UID、およびMAC1(VMKEY <sub>n</sub> に基づく)を含むMSG1がVALMODからホストへ送られる。	

(33)

生成されるもの
MAC 1
RNKEY
VMSEED <sub>n+1</sub>
VMKEY <sub>n+1</sub>
UAP
UAKKEY
VMID、UAP ( VMSEED <sub>n</sub> ( UVP )、 VMKEY <sub>n</sub> に基づく )、NEWKEY ( RNK EY、UAKKEY に基づく )、およびMAC 2 ( VMKEY <sub>n</sub> に基づく ) を含むMSG 2 がホスト からVALMODへ送られる。
入力されたUPWより
生成されるもの
UVP
UAP
UAKKEY
RNKEY
VMSEED <sub>n+1</sub>
VMKEY <sub>n+1</sub>

(34)

H I I D、V M I D、V M P A R、U I D、およびM A C 3 ( V M K E Y <sub>n+1</sub> に基づく)を含むM S G 3がV A L M O Dからホストへ送られる。

V A L M O DおよびホストはいずれもV M S E E D <sub>n+1</sub>およびV M K E Y <sub>n+1</sub>を記憶する。

どの段階においてもV A L M O Dおよびホストの部外者が利用できるV M S E E D <sub>n+1</sub>およびV M K E Y <sub>n+1</sub>は存在しない。

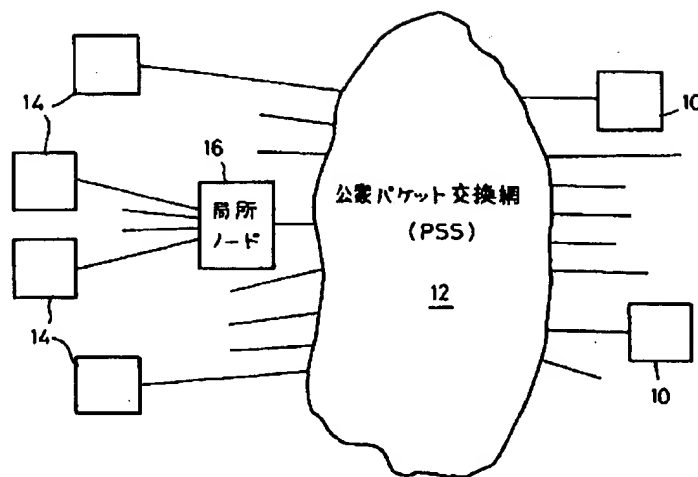
#### ( 発 明 の 効 果 )

以上説明したように本発明によれば、メッセージ交換のたびごとに自動的にキーの更新がなされるので、従来に比べてより優れた安全保護システムが提供される。

#### 4. 図面の簡単な説明

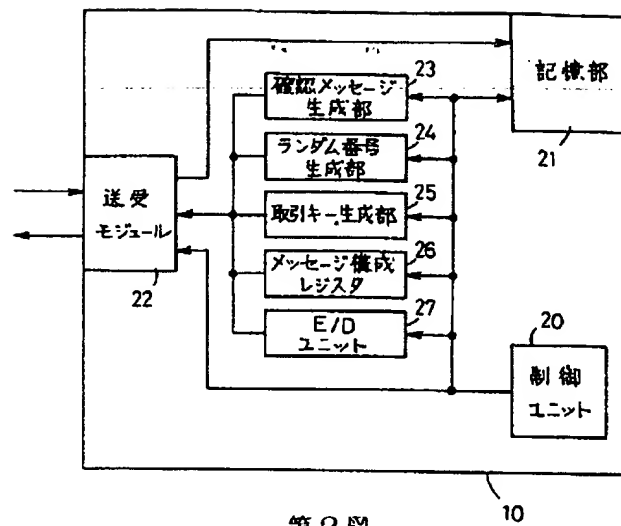
第1図はホームバンキングデータ通信システムを簡略的に示すブロック図、第2図はホストプロセッサの構成例を示すブロック図、第3図は検証モジュールの構成例を示すブロック図である。

(35)

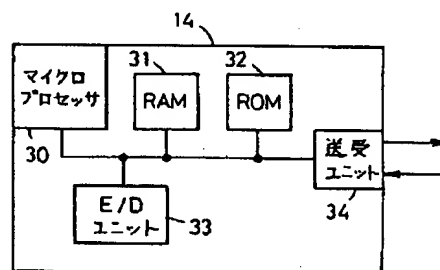


10 … ホストプロセッサ  
14 … 端末機

第1図



第2図



第3図

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.